第 38 卷第 3 期
录用定稿
计算机应用研究
Application Research of Computers
Vol. 38 No. 3
Accepted Paper

IDDS：一种双链结构传染病数据共享区块链模型 *

刘　炜[a, c]，李　阳[b, c]，田　钊[a]，彭宇飞[b, c]，佘　维[a, c†]

(郑州大学 a. 软件学院; b. 信息工程学院; c. 互联网医疗与健康服务河南省协同创新中心，郑州 450000)

摘　要：现有传染病预防信息系统在工作过程中存在数据难以流通和共享等问题。为了解决这些问题，借由区块链的去中心化、不可窜改和集体维护等特点，提出了一个基于 DPoS 共识算法的传染病数据共享模型 IDDS，该模型采用双链结构作为区块链架构，提高了工作效率；结合 IPFS 获得大容量存储空间，解决了区块数据存储面临的空间问题，保障了数据存储稳定性与共享安全性；提出了疾病防控共识算法，实现了传染病数据共享模型的高效运行。此外，通过与其他数据共享模型的对比，突出了该模型在数据存储与共享安全等方面的优势。

关键词：区块链；双链；DPoS；IPFS；数据共享

中图分类号：TP393　　doi: 10.19734/j.issn.1001-3695.2020.01.0031

IDDS: double-chain structure infectious disease data sharing blockchain model

Liu Wei[a, c], Li Yang[b, c], Tian Zhao[a], Peng Yufei[b, c], She Wei[a, c†]

(*a. School of Software*, *b. School of Information Engineering*, *c. Collaborative Innovation Center for Internet Healthcare*, *Zhengzhou University*, *Zhengzhou* 450000, *China*)

Abstract: The infectious disease prevention information system has the problems that data is difficult to circulate and share between monitoring systems. To solve these problems, this paper based on Delegated Proof of Stake consensus algorithm combined with blockchain technology proposed an Infectious Disease Data Sharing model. By virtue of the characteristics of the blockchain, such as decentralization, non-tampering and collective maintenance, double-chain be used as the blockchain architecture, which improves the work efficiency. Combined with Inter-Planetary File System, large capacity storage space is obtained, which solves the space problem faced by block data storage and ensures the stability and sharing security of data storage. A consensus algorithm for disease prevention and control to realize the efficient operation is proposed by this paper. In addition, by comparing with other data sharing models, the advantages of this model in data storage and sharing security are highlighted.

Key words: blockchain; double chain; delegated-proof-of-stake; inter-planetary file system; data sharing

0　引言

随着信息化时代的发展，世界各国均已针对“区块链+医疗”开展研究并进行广泛应用[1~10]。区块链采用链式存储结构，具有去中心化、不可窜改、集体维护等特点，可以很好的解决现有传染病预防控制信息系统存在的数据共享安全等问题。传染病预防信息系统对于传染病的监测、预防起着非常重要的作用。我国在 2003 年首次提出并建设了一套传染病网络直报信息平台——中国疾病预防控制信息系统[11]，极大地提高了报告的及时性和完整性。但在实践过程中，暴露出了现有传染病预防信息系统存在的一些问题，如在数据传输过程中，容易发生隐私数据泄露，存在安全风险；系统与系统之间的数据无法较好的进行流通，影响了疫情报告的有效性和即时性。

区块链与医疗领域结合已有许多先例，如 Azaria 等人提出的 MedRec 健康记录管理系统，利用区块链的独特属性来保存和共享电子健康信息档案[12]；Xia 等人提出的 BBDS 电子健康记录和共享系统[13]为敏感信息提出了一个安全、可扩展的访问控制系统；他们提出的另一个 MeDShare 系统[14]解决了医疗大数据在无信任环境中医疗数据共享问题，其用于在云服务提供商之间共享医疗数据，同时提供数据访问控制、来源和审计；文献[15]描述了一个分散的个人数据管理系统，确保用户拥有和控制他们的数据，并且实现了一个将区块链转换为自动访问控制管理器的同时不需要信任第三方的协议；文献[16]提出了一个管理和共享癌症患者护理的 EMR 数据的框架，可以确保数据的隐私、安全、可用性以及对 EMR 数据的细粒度访问控制，显著缩短了 EMR 共享的周转时间，改善了医疗保健决策，降低了总体成本；Peterson 等人提出了基于区块链的方法[17]来共享患者数据，在数据共享网络中可以高效和安全地共享医疗信息；Linn 等人描述了一个基于区块链的健康记录访问控制管理器[18]，用户可以完全拥有其数据的权限并可以分配权限给不同的人。从目前国内外的研究可以看出，已有区块链与医疗数据共享结合的先例，但现有的区块链数据共享模型中，大多为采用单链结构私有链，工作效率低，节点权限难以控制，数据存储空间也较小，难以满足传染病数据共享平台的数据存储、节点权限控制等需求。

针对以上问题，本文提出一种基于 DPoS 共识算法的传染病数据共享模型，利用联盟链的双链结构提高工作效率，结合 IPFS(Inter-Planetary File System)存储大容量医疗数据，改进 DPoS 共识算法，提高共识的安全性和投票节点积极性。

收稿日期：2020-01-16；**修回日期：**2020-04-13　**基金项目：**国家重点研发计划资助项目(2018YFB1201403)；河南省高等学校重点科研资助项目(20A520035)；河南省高等学校青年骨干教师资助项目(2019GGJS018)；赛尔网络下一代互联网技术创新资助项目(NGII20190707)

作者简介：刘炜(1981-)，男，河南安阳人，副教授，博士，主要研究方向为无线网络、区块链，智慧医疗；李阳(1998-)，男，山东菏泽人，硕士研究生，主要研究方向为区块链，互联网医疗；田钊(1985-)，男，河南荥阳人，讲师，博士，主要研究方向为信息安全、人工智能、智能交通；彭宇飞(1994-)，女，河南三门峡人，硕士研究生，主要研究方向为区块链，信息安全；佘维(1977-)，男(通信作者)，湖南常德人，副教授，硕导，博士，主要研究方向为区块链、能源互联网、互联网医疗(wshe@zzu.edu.cn).

1 相关技术

1.1 区块链

区块链本质上是一种分布式数据库，由众多的数据区块按时间顺序连接而成[19~24]。每个数据区块均由区块头(Header)和区块体(Body)两部分组成：a)Header 包含的主要信息是上一区块的哈希散列值，用来实现区块的连接，保证了链式结构的完整性和可追溯性；b)Body 包含一段时间内所有的交易信息，这些交易通过 Merkle 树的哈希过程生成唯一的 Merkle 根并记录在 Header 中。

区块链主要有三种形式：公有链、联盟链和私有链。公有链具有完全去中心化、全网公开、数据透明等特点，分布式系统中所有节点均可参与链上数据的读写、验证和共识过程，并通过概率性共识机制(例如 PoW、PoS)获得相应的经济激励。由于公有链的这些性质，使其在金融领域和数字货币方面得到了广泛的应用。私有链具有工作效率高、隐私保护性好、交易成本低等特点，但相比较于公有链和联盟链，其去中心化程度较低，对于节点权限控制严格。综上所述，由于医疗服务系统的特殊性，公有链与私有链并不适用于构建传染病数据共享模型。

联盟链是一种有限去中心化区块链架构，系统中各个节点通常有与之对应的实体机构组织，通过授权之后才能加入或退出网络。各节点可根据具体的需求组成不同的利益联盟，共同维护联盟链系统的正常运转。联盟链在交易效率、隐私安全性等方面表现良好，同时可以更灵活的接入节点。

1.2 授权股份证明(DPoS)

授权股份证明(DPoS，Delegated Proof of Stake)是一种投票机制，由全网中所有持有代币的节点进行投票，得票最多且愿意成为打包节点的前 101 个节点成为授权节点，进入打包队列，节点持有的代币相当于股份，持有代币越多，节点投票所占权重也越大。节点投票选出的 101 个节点将按照顺序对区块链中区块进行打包产生区块，打包过程将获得代币奖励。如果授权节点错过打包区块，系统将从打包队列中将其剔除。

DPOS 算法可以将区块生成时间从 10 分钟减少至数秒，实现了区块生成效率的成倍增加，使得交易确认速度加快，但其对于故障及恶意节点的处理仍存在许多困难，存在安全隐患。

2 传染病数据共享模型 IDDS

本文使用双链结构区块链作为模型架构，提出了一种基于 DPoS 共识算法的传染病数据共享模型 IDDS(Infectious Disease Data Share model)，解决系统数据共享安全问题，使得监测系统间的数据共享安全得以保证。

2.1 IDDS 架构

传染病数据共享模型 IDDS 六元组定义如下：

$$\text{IDDS} = (HN, DN, EN, C_{IDDS}, , \text{DPCC}, T)$$

其中：$HN = \{hn_i \mid i \in N^+\}$ 为医疗机构节点有限集；$DN = \{dn_i \mid i \in N^+\}$ 为疾控中心节点有限集；$EN = \{en_i \mid i \in N^+\}$ 为边缘节点有限集；CIDDS 是 IDDS 区块链架构，包含快速病情收集链，实时病情分析链和用户系统三层；DPCC(Disease Prevention and Control Algorithm)为疾病防控共识算法。$T = \{t_f \mid t_f \in HN \times EN \cup EN \times DN, f \in N^+\}$ 是各个节点之间交易的有限集。其中，$HN \times EN$ 是 HN 与 EN 之间交易的有限集，$EN \times DN$ 是 EN 与 DN 之间交易的有限集。

IDDS 模型采用双链架构，共分为三层，分别为用户系统(*Sys*)、实时病情分析链 Slow chain(*SC*)、快速病情收集链 Fast Chain(*FC*)，如图 1 所示。

a) *FC*：IDDS 双链结构中的 Fast Chain，为快速病情收集链，*FC* 中包含区块 fast block(*fb*)。*fb* 中存储病情数据摘要，由各个医疗机构主动生成并上传。

b) *SC*：IDDS 双链结构中的 Slow Chain， 为实时病情分析链，*SC* 中包含区块 slow block(*sb*)，对 *fb* 中的病情数据分析后生成的数据报告将被存储在 *sb* 中。

c) *Sys*：获取 *sb* 中的疫情分析报告，监控各地区疫情的实时数据，对于可能发生疫情的地区进行预警。

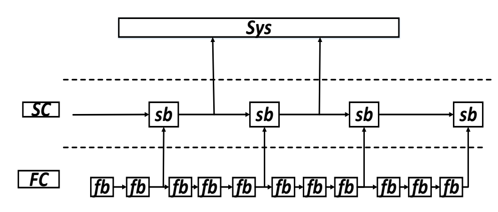


图 1 IDDS 基础架构图

Fig. 1 Basic architecture of IDDS

在双链结构中，*FC* 链和 *SC* 链通过基于 hash 值的方式锚定连接。为了实现对大容量数据存储访问，减轻区块链打包压力，IDDS 模型与 IPFS 相结合，将疫情数据 *data* 存储在 IPFS 数据库中，*FC* 链区块 *fb* 中只存储 *data* 在 IPFS 中的 hash 值与数据摘要等信息；*SC* 链中节点通过智能合约对 *FC* 中区块所对应的 IPFS 上疫情数据信息 *data* 进行分析，将分析结果存储在 *SC* 链的区块 *sb* 上，结果公开可供 *Sys* 查看，使得疫情分析结果与隐私数据隔离，增强了对疫情数据安全性和隐私性的保护。

IDDS 模型中的节点分为 3 类：医疗机构节点(*hn*)、疾控中心节点(*dn*)、边缘节点(*en*)。由这三类节点组成了 IDDS 区块链模型。*hn*、*dn*、*en* 节点关系如图 2 所示。

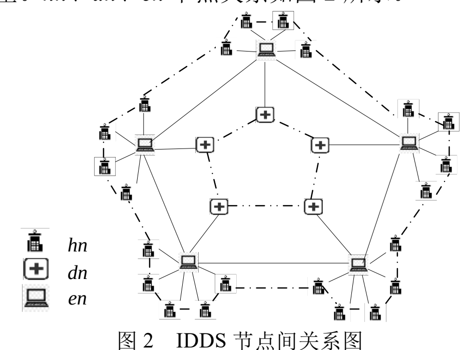


图 2 IDDS 节点间关系图

Fig. 2 IDDS node relationship diagram

节点各自职能定义如下：

a) *hn*：医疗机构节点，用于上传实时疫情数据，负责 *FC* 区块打包。

b) *dn*：疾控中心节点，负责 *SC* 区块打包。

c) *en*：边缘节点，用于连接 *hn* 与 *dn*，由一部分疾控中心节点作为边缘节点。

本文提出的 CIDDS 拓扑结构示意图如图 3 所示。在该方案中，每个医疗机构及疾病控制管理中心都具有其对应的节点。*hn* 与 *dn* 分别属于 *FC* 和 *SC*，由 *en* 进行连接。其中 *hn* 属于 *FC*，而 *dn* 属于 *SC*。IDDS 模型拓扑结构如图 3 所示。

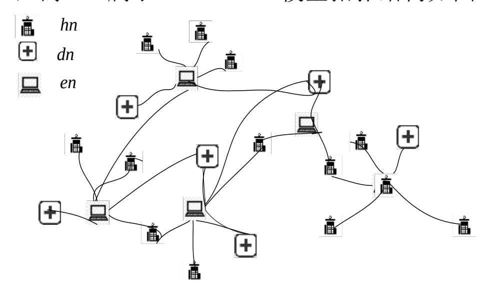


图 3 IDDS 拓扑结构示意图

Fig. 3 Schematic diagram of IDDS topology

2.2　数据传输与处理

在 IDDS 模型中，*hn* 调用智能合约将疫情数据(*data*)加密后上传至 IPFS 数据库，IPFS 对 *data* 进行加密后返回的 hash 值与病情数据摘要一同保存在 *fb* 中；每生成 3 个 *fb*，*dn* 将通过 *fb* 中的 hash 值从 IPFS 中索引到对应的数据，对数据处理后得到分析结果，打包到 *sb* 中，最终 *sb* 中的分析结果将被上传至 *Sys* 中。

IDDS 模型的数据流图如图 4 所示。此时各个医疗机构上传的疫情数据经由智能合约分析后被上传至疾病控制管理中心。由现行传染病爆发判定标准[25]，当发生传染病疫情时，该方案建立了基于区块链的信息共享模型，确保了疫情数据传输过程的即时有效，由智能合约分析得到有效数据后将数据上传至疾病控制管理中心，实现对传染病疫情的实时监测。

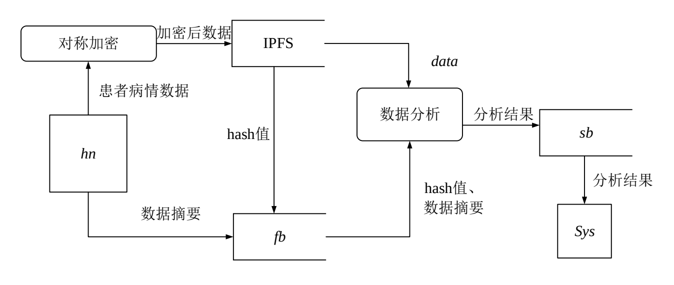


图 4　IDDS 数据流图

Fig. 4　IDDS data flow diagram

2.3　疾病防控共识算法 DPCC

针对共识过程中恶意节点和投票积极性等问题，本文在 DPoS 共识机制的基础上，从信誉积分、投票机制、奖励与阈值等三个方面提出了一种新的改进方案——疾病防控共识算法 DPCC(Disease Prevention and Control Algorithm)，解决了 DPoS 算法中存在的对恶意节点处理不及时，节点投票积极性不高等问题。

2.3.1 信誉积分 Reputation Credit

在 DPCC 中，提出了信誉积分 *RC*(Reputation Credit)的概念。*RC* 作为一种节点评价指标，用于评价节点的好坏。信誉积分越高，表示节点在之前的区块打包过程中表现良好，值得信任；信誉积分低则表示节点可能为恶意节点。对于表现良好的节点，将根据其对于区块打包的贡献程度，分别奖励其不等的 *RC*。而对于故障节点或恶意节点，无法完成打包操作或打包错节点时，DPCC 将扣除节点的 *RC*，同时为其投赞成票的节点 *RC* 也将被扣除。扣除 *RC* 将意味着节点成为打包节点的难度加大，在为其他节点投票时所占权重更小，无法获得更多的奖励。

2.3.2 投票机制

在 DPoS 共识算法中，通过计算该节点获得的投票数来选择进入打包队列(*hlist*)的节点。DPCC 中对传统的 DPoS 共识算法的投票机制进行了改进，普通节点向自己所信任的节点投赞成票 *PV*(Positive Vote)，而向信任的节点投反对票 *DV*(Disagree Vote)，在选举打包节点时即预防恶意节点进入 *hlist*。

本文结合信誉积分提出了一种新的计算节点总得票数(*Total*)的公式：

$$Total = \left(\sum_{1}^{m} PV_i - \sum_{1}^{n} DV_i\right)/(m+n) + RC \tag{1}$$

在式(1)~(3)中，PV_i 为投 *PV* 的第 i 个节点所拥有的 *RC* 值，DV_i 为投 *DV* 的第 i 个节点所拥有的 *RC* 值，*m* 为向该节点投 *PV* 的节点个数，*n* 为向该节点投 *DV* 节点个数。通过求出所有投赞成票节点的 *RC* 值之和，减去向该节点投反对票节点的 *RC* 值之和后求平均值，与该节点自身所拥有的 *RC* 相加，得到 *Total*，取 *Total* 值最高的前百分之 10 的节点进入 *hlist*，对区块进行打包。当 *Total* 值小于 0 时，将 *Total* 值计为 0。在一轮投票中，对节点所获 *Total* 值由高到低进行排序，根据 *Total* 的高低，将节点分为不同类型：

a) 打包节点：*Total* 值为最高的前 10%的节点；

b) 普通节点：*Total* 值位于由高到低 10%到 90%的节点；

c) 恶意节点：*Total* 值位于最后 10%的节点。

2.3.3 奖励与阈值

DPoS 算法对于成功打包区块的节点和投票选举这些打包节点的普通节点会给予一定的奖励 Reward(*Re*)。这些奖励可以增加普通节点的投票积极性，避免投票率低和无人投票等问题。其他节点投票时通过该节点在之前打包过程中的表现可以自由选择赞成票还是反对票，当其投给赞成票的节点进入 *hlist* 并成功打包节点，该节点将根据信誉积分的多少获得相应的奖励；相应的，当节点为恶意节点时，向该节点投反对票的节点将得到奖励，用以激励节点向潜在的恶意节点投反对票。

随着节点 *RC* 的增加，节点自身的权重也越来越大，所以当 *RC* 增加到一定值时，需要削减以平衡该节点与网络中其他节点的关系。设 *α* 为 *RC* 阈值，*β* 为 *RC* 最大值，Re_i 为参与投票或进行打包的第 i 个节点所得奖励。式(2)以成功打包区块的打包节点为例，考虑了节点 *RC* 值小于 *α* 和处于 *α* 到 *β* 之间时，节点所获 *Re*：

$$Re_i = \begin{cases} PV_i / (\sum_{1}^{m} PV_i + RC)*Re & RC \le \alpha \\ PV_i / (\sum_{1}^{m} PV_i + RC)*Re*(\alpha / RC) & \alpha < RC < \beta \end{cases} \tag{2}$$

当节点 *RC* 达到最大值 *β* 时，节点 *RC* 值将被重置为阈值 *α*，即使得节点在 *hlist* 的选举中保持优先，又维护了网络中各节点的被选举公平性，防止了节点 *RC* 值持续升高，保证了其他节点的选举积极性。

节点信誉积分越高，表示该节点在区块打包过程中的表现越好，其他节点投票给它更有可能获得 *Re*，避免惩罚；而它向其他节点投票时，所占权重越大，越具有代表性。

2.3.4 信誉积分惩罚机制

而当节点为故障节点或恶意节点，并未成功打包区块时，该节点将被扣除信誉分并将其从 *hlist* 中剔除，设 *γ* 为惩罚系数，*PU* 为节点被惩罚时所扣除的 *RC* 值，向恶意节点投赞成票选举其进入 *hlist* 的节点及向成功打包区块的打包节点投反对票的节点将被扣除 *PU*，以向恶意节点投 *PV* 为例，如式(3)所示。

$$PU = \begin{cases} PV_i / \sum_{1}^{n} PV_i * \gamma * Re & RC > \theta \\ 0 & RC \le \theta \end{cases} \tag{3}$$

在 DPCC 共识算法中，将按照式(1)得到区块链网络中所有节点的 *Total* 值，对其进行排序，取最高的前百分之 10 的节点组成 *hlist*，对区块进行打包。若 *hlist* 中的节点成功打包区块，该节点及为其投 *PV* 的节点将获得相应 *Re*；若 *hlist* 中的节点为恶意节点，无法正常打包区块，由式(3)扣除该节点及为其投赞成票节点的 *RC*，扣除值为 *PU*。设 *θ* 为 *RC* 最小值，当 *RC* 被扣除至 *θ* 以下时，*RC* 值将不再变化。

以 *fb* 的打包过程为例，DPCC 工作过程如下所示。

```
输入:疫情数据
输出: fb
由式(1)计算得 Total 值序列
将 Total 值降序排序
取前百分之 10 节点为组成 hlist;
while (i<hlist.length()){ //对 hlist 列表进行遍历
if(hn_i 无法正常打包区块){
```

```
/*若 hlist 中第 i 个节点为恶意节点*/
由式(2)(3)计算得 Re_i,PU;/*计算相应 Re_i,PU*/
RC=RC-PU;   //扣除恶意节点及为该节点投赞成票
PV_i=PV_i-PU;  //的节点信誉积分
DV_i=DV_i+Re_i; //奖励向恶意节点投反对票的节点
将恶意节点从 hlist 中踢除;
i←i+1;
}
hn_i 对区块进行打包;
由式(2)(3)计算得 Re_i,PU;/*计算相应 Re_i,PU*/
RC=RC+Re;    //打包节点获得奖励，信誉值增加
PV_i=PV_i+Re; //奖励向打包节点投赞成票的节点
DV_i=DV_i-PU; //惩罚向打包节点投反对票的节点
返回 fb
}
```

3　实验验证及分析

通过仿真实验对 DPCC 共识算法进行模拟并对其有效性及安全性进行分析。实验基于 python 语言模拟 100 个网络节点进行投票，其中设置恶意节点比率为百分之 10， α 为 80，β 为 100， θ 为 20，共进行了 200 轮。

3.1　投票节点总得票数的合理性验证

由于节点所拥有的信誉积分不同，投票阶段所得到的赞成票和反对票也不同。实验主要分析在同一轮投票过程中，拥有不同 *RC* 的节点所获得的 *PV* 以及 *Total* 比较，实验结果如图 5 所示。

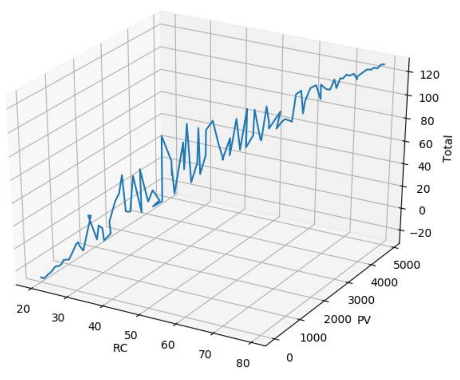


图 5　节点 Total 值变化趋势图

Fig. 5　Total value change trend graph of nodes

由投票结果可以看出，当节点的 *RC* 值较小时，所得到的赞成票较少，因此 *Total* 值也越少。而随着节点 *RC* 值的增大，节点得到的 *PV* 也随之增加，拥有最多 *RC* 的节点所得到 *Total* 值最多，即信誉积分越多的节点进入 *hlist* 的机会也越大。在投票过程中，节点也会倾向于向 *RC* 值大的节点进行投票，有助于自己获得更多 *Re*。节点 *Total* 值不会一直增加，当节点自身的 *RC* 达到最大值时会被重置为阈值，节点 *Total* 值也会随之下降。

3.2　多轮投票中不同类型节点的比较

本文比较了在多轮投票中，打包节点、普通节点与恶意节点所得票数的不同。本文记录了 200 次投票中普通节点与恶意节点的得票数，通过绘制折线图来体现在 200 次投票过程中不同类型节点所得票数趋势，如图 6 所示。

通过对比分析，在多轮投票过程中，打包节点所得票数明显逐渐升高并在接下来投票过程中保持领先，表示打包节点由于自身表现稳定，无不良记录，使得其他节点更倾向于投给它来获得 *Re*；普通节点通过正确的投票，整体呈现稳定上升趋势；而对于恶意节点，初始时与普通节点所获票数相似，随着轮数的增加，其他节点将向恶意节点投反对票来获得 *Re*，恶意节点所得票数逐渐减少，有效防止了恶意节点进入 *hlist*。

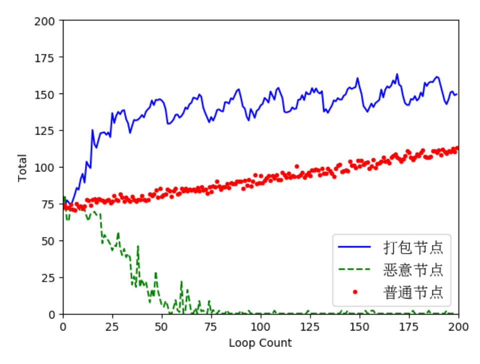


图 6　200 轮投票结果

Fig. 6　200 rounds of voting results

3.3　多轮投票中打包节点 RC 值变化趋势

在多轮投票中，打包节点由于表现良好，*RC* 值将持续升高，达到阈值 80 后，根据式(2)，将改变增加速度直到达到最大值 100。达到最大值后，系统将节点 *RC* 重置为阈值，*RC* 继续按照式(2)增加，达到最大值之后将再次被重置，以循环 50 轮为例，如图 7 所示。

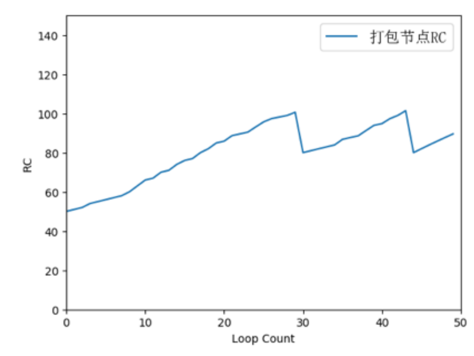


图 7　打包节点 RC 变化趋势图

Fig. 7　RC change trend graph of package nodes

3.4　模型分析

本文从共识机制、安全性和效率等方面与其他模型进行了对比，如表 1 所示，IDDS 模型采用基于联盟链的双链结构可以减轻主链压力，提高系统工作效率，更好的实现数据安全共享。同时，分析了当前传染病预防信息系统面临的隐私安全、数据存储和工作效率等方面的问题以及 IDDS 所具有的优势(如表 2 所示)。当面临大容量存储问题时，IDDS 模型结合 IPFS 文件系统来实现对大规模数据的存储及便捷访问，有效解决已有基于区块链模型存在的区块容量小等问题；节点将数据存储在 IPFS 中，IPFS 返回的 hash 值被存储在 *FC* 的区块 *fb* 中，可以有效保护医疗数据泄露和隐私安全；双链架构保证了区块的打包效率，DPCC 共识算法使得在数据传输及区块打包过程中有效减少了资源浪费。但本模型仍有需要改进的地方，在未来的工作中将对模型做进一步的改进，提高工作效率，完善共识算法。

4　结束语

随着区块链技术的发展，区块链与医疗领域的结合将越来越多，医疗领域的隐私安全、数据共享等问题已经得到越来越多的关注。本文研究了现有传染病预防信息系统中存在的数据难以共享等问题，提出了具有去中心化、工作效率高、存储空间大的传染病数据共享模型，满足越来越多的医疗数据安全共享与大量医疗数据存储需求。本文希望为未来的智慧医疗研究提供新的思路，推动智慧医疗与区块链的结合，共同向前发展。

表 1 IDDS 与其他解决方案对比

Tab. 1 IDDS compare with other solutions

	共识机制	安全性	效率
IDDS	DPCC	在 DPoS 的基础上对其进行了改进，提高节点活跃度，剔除恶意节点，确保系统安全性	效率高
MedRec	PoW	-	效率低
MeDShare	-	通过智能合约和访问控制机制跟踪数据行为，并在检测到违反数据权限行为时撤销访问权限	元组的大小以及数据的处理和匿名化都会增加延迟，注重安全性

表 2 当前面临的问题及 IDDS 解决方案

Tab. 2 Current problems and solutions for IDDS

类型	面临问题	IDDS 应对方法及分析
隐私和安全	可窜改 数据泄露 黑客攻击和数据安全	采用基于区块链的底层架构，利用区块链的去中心化、不可窜改等特点保证数据安全；DPCC 共识算法有效对恶意节点进行了处理，保障了 IDDS 的有效运行
数据存储	区块容量小 访问便捷性 大容量数据存储	将数据存储在 IPFS 文件系统中，实现了对大规模数据的存储及便捷访问
工作效率	所需时间长 浪费算力资源	IDDS 采用双链架构提高工作效率； DPCC 相较于 PoW 共识算法减少了资源浪费

参考文献：

[1] Li C, Cao Y, Hu Z, *et al.* Blockchain-based Bidirectional Updates on Fine-grained Medical Data [C]// 2019 IEEE 35th International Conference on Data Engineering Workshops (ICDEW) . IEEE, 2019: 22-27.

[2] Chen Y, Ding S, Xu Z, *et al.* Blockchain-based medical records secure storage and medical service framework [J]. Journal of medical systems, 2019, 43 (1): 5.

[3] Jamil F, Hang L, Kim K H, *et al.* A Novel Medical Blockchain Model for Drug Supply Chain Integrity Management in a Smart Hospital [J]. Electronics, 2019, 8 (5): 505.

[4] Patel V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus [J]. Health informatics journal, 2019, 25 (4): 1398-1411.

[5] Tian H, He J, Ding Y. Medical data management on blockchain with privacy [J]. Journal of medical systems, 2019, 43 (2): 26.

[6] Dwivedi A D, Srivastava G, Dhar S, *et al.* A decentralized privacy-preserving healthcare blockchain for IoT [J]. Sensors, 2019, 19 (2): 326.

[7] de Oliveira M T, Reis L H A, Carrano R C, *et al.* Towards a blockchain-based secure electronic medical record for healthcare applications [C]// ICC 2019-2019 IEEE International Conference on Communications (ICC) . IEEE, 2019: 1-6.

[8] Shen M, Deng Y, Zhu L, *et al.* Privacy-preserving image retrieval for medical iot systems: A blockchain-based approach [J]. IEEE Network, 2019, 33 (5): 27-33.

[9] Cheng X, Chen F, Xie D, *et al.* Design of a Secure Medical Data Sharing Scheme Based on Blockchain [J]. Journal of Medical Systems, 2020, 44 (2): 52.

[10] Wu S, Du J. Electronic medical record security sharing model based on blockchain [C]// Proceedings of the 3rd International Conference on Cryptography, Security and Privacy. 2019: 13-17.

[11] 熊玮仪，冯子健. 中国传染病监测的发展历程、现状与问题 [J]. 中华流行病学杂志, 2011, 32 (10): 957-960. (Xiong Weiyi, FENG Zijian, The development, status and problems of infectious disease monitor in China [J] , Chinese Journal of Epidemiology, 2011, 32 (10): 957-960.)

[12] Azaria A, Ekblaw A, Vieira T, *et al.* Medrec: Using blockchain for medical data access and permission management [C]// 2016 2nd International Conference on Open and Big Data (OBD) . IEEE, 2016: 25-30.

[13] Xia Q, Sifah E B, Smahi A, *et al.* BBDS: Blockchain-based data sharing for electronic medical records in cloud environments [J]. Information, 2017, 8 (2): 44.

[14] Xia Q I, Sifah E B, Asamoah K O, *et al.* MeDShare: Trust-less medical data sharing among cloud service providers via blockchain [J]. IEEE Access, 2017, 5: 14757-14767.

[15] Zyskind G, Nathan O. Decentralizing privacy: Using blockchain to protect personal data [C]// 2015 IEEE Security and Privacy Workshops. IEEE, 2015: 180-184.

[16] Dubovitskaya A, Xu Z, Ryu S, *et al.* Secure and trustable electronic medical records sharing using blockchain [C]// AMIA annual symposium proceedings. American Medical Informatics Association, 2017, 2017: 650.

[17] Peterson K, Deeduvanu R, Kanjamala P, *et al.* A blockchain-based approach to health information exchange networks [C]// Proc. NIST Workshop Blockchain Healthcare. 2016, 1: 1-10.

[18] Linn L A, Koo M B. Blockchain for health data and its potential use in health it and health care related research [C]// ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST. 2016: 1-10.

[19] Cong L W, He Z. Blockchain disruption and smart contracts [J]. The Review of Financial Studies, 2019, 32 (5): 1754-1797.

[20] 王继业，高灵超，董爱强，等. 基于区块链的数据安全共享网络体系研究 [J]. 计算机研究与发展, 2017, 54 (04): 742-749. (Wang Jiye, Gao Lingchao, Dong Aiqiang, *et al.* Block chain based data security sharing network architecture research [J]. Journal of Computer Research and Development, 2017, 54 (4): 742-749.)

[21] Dagher G G, Mohler J, Milojkovic M, *et al.* Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology [J]. Sustainable Cities and Society, 2018, 39: 283-297.

[22] 袁勇，王飞跃. 区块链技术发展现状与展望 [J]. 自动化学报, 2016, 42 (4): 481-494. (Yuan Yong, Wang Feiyue. Blockchain: the state of the art and future trends [J]. Acta Automatica Sinica, 2016, 42 (4): 481-494.)

[23] 袁勇，王飞跃. 平行区块链：概念、方法与内涵解析 [J]. 自动化学报, 2017, 43 (10): 1703-1712. (Yuan Yong, Wang Feiyue. Parallel

blockchain: concept, methods and issues [J]. Acta Automatica Sinica, 2017, 43 (10): 1703-1712.)

[24] Leng K, Bi Y, Jing L, *et al.* Research on agricultural supply chain System with double chain architecture based on blockchain technology [J]. Future Generation Computer Systems, 2018, 86: 641-649.

[25] 徐春华, 马家奇. 现行传染病爆发判定标准与方法 [J]. 疾病监测, 2007 (11): 777-780. (XU Chunhua, MA Jiaqi, Current standards and methods to judge the outbreak of infectious diseases [J] , Disease Surveillance, 2007 (11): 777-780.)